



Template Document for the Interim Final Rule

33 CFR 105.405

POC: Facility Security Officer

Facility Name and Address

Business Phone

24 Hour Contact Number

This cover page is a recommendation to ease contact when an emergency occurs, though the regulations cover many details they do not require this information to be on the cover of the manual.

IT IS VERY IMPORTANT to remember that the information in this plan must be protected from public release as sensitive security information in accordance with 49 CFR part 1520

First Draft 21AUG03.

Facility Security Plan

Please note: that in the body of this template document there is text in this format (green and italic) which is either a notes on regulatory interpretation or is an actual citation notes from the interim final rule.

The information in other styles is an example of the content the Coast Guard Plan Examiners will be looking for, prior to approving the plan.

33 CFR 105.400 calls for the Facility Security Officer (FSO) to ensure that a Facility Security Plan (FSP) is developed and implemented at each facility for which he or she is FSO. General content requirements are found under this citation. (Also the web address for electronic submission of a FSP is given : <http://www.uscg.mil/HQ/MSC>)

33 CFR 105.405 calls for the FSP to follow the order given below in the Table of Contents or for there to be a cross-referenced index. This is similar to other plans mandated by regulation. The specifics of some facilities make the consolidation of information and indexing easier for the FSO.

Also a part of this subsection, which is not specifically considered in the template, is the possibilities of waivers, exceptions or alternative program approval. These portions of the regulations are for research by the FSO or other facility representation. To make such applications is possible but will require the proverbial “case by case” review by the cognizant Captain of the Port.

The FSP will address itself to the requirements Subpart B of 33 CFR 105. This is the section where the list of responsibilities and actions to be taken has been codified.

These interim regulations use definitions from 33 CFR 101 as well as adding definitions that are specific to the facilities requirements.

Facility Security Plan

Of particular interest is the section on applicability, 33 CFR 105.105:

(a) The requirements in this part apply to the owner or operator of any U.S.:

- (1) Facility subject to 33 CFR parts 126, 127, or 154;*
- (2) Facility that receives vessels certificated to carry more than 150 passengers;*
- (3) Facility that receives vessels subject to the International Convention for Safety of Life at Sea, 1974, or that are commercial vessels subject to subchapter I of title 46, Code of Federal Regulations, greater than 100 gross register tons on international voyages, including vessels solely navigating the Great Lakes; or*
- (4) (Fleeting facility that receives barges carrying, in bulk, cargoes regulated by subchapters D and O of chapter I, title 46, Code of Federal Regulations or Certain Dangerous Cargoes.*

(b) An owner or operator of any facility not covered in paragraph (a) of this section is subject to parts 101 through 103 of this subchapter.

(c) This part does not apply to the owner or operator of the following U.S. facilities:

- (1) A facility owned and operated by the U.S. that is used primarily for military purposes.*
- (2) An oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if:*

- (i) The facility is engaged solely in the exploration, development, or production of oil and natural gas; and*
- (ii) The facility does not meet or exceed the operating conditions in § 106.105 of this subchapter;*

(3) A facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if:

- (i) The facility is engaged solely in the support of exploration, development, or production of oil and natural gas; and*
- (ii) The facility transports or stores quantities of hazardous materials that do not meet and exceed those specified in 49 CFR 172.800(b)(1) through (6); or*
- (iii) The facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154;*

(4) A mobile facility regulated by 33 CFR part 154; or

(5) An isolated facility that receives materials regulated by 33 CFR parts 126 or 154 by vessel due to the lack of road access to the facility and does not distribute the material through secondary marine transfers.

Facility Security Plan

TABLE OF CONTENTS

- 1. Security administration and organization**
- 2. Personnel Training**
- 3. Drills and Exercises**
- 4. Records and Documentation**
- 5. Response to Change in MARSEC Level**
- 6. Procedures for interfacing with vessels**
- 7. Declaration of Security (DOS)**
- 8. Communications**
- 9. Security systems and equipment maintenance**
- 10. Security measures for access control, including designated public access areas**
- 11. Security measures for restricted areas**
- 12. Security measures for handling cargo**
- 13. Security measures for delivery of vessel stores and bunkers**
- 14. Security measures for monitoring**
- 15. Security incident procedures**
- 16. Audits and security plan amendments**
- 17. Facility Security Assessment (FSA) report**
- 18. Facility Vulnerability and Security Measures Summary**

Facility Security Plan

PLAN APPROVAL AND REVIEW

33CFR105.410 calls for the submission of the FSP to the cognizant Captain of the Port (COTP) where it will be examined and a letter will be returned approving, specifying conditions of approval or disapproval with corrections required. Final approval shall be for a period of five years barring major modifications to the plan. A copy of the approval letter shall be available for inspection as required by 33 CFR 105.120.

Approved by: **U.S. Coast Guard**
 Marine Safety Office (name of office)

A copy of the original letter or the location where it is kept on the facility could be placed here.

Review Dates:

Keeping track of dates of review and submission of updates is always a good idea. Section 4 calls for a letter documenting the audit to be filled and filed by the FSO. As these letters may be filed elsewhere a review page like this one, kept in the plan may aid in keeping track of the current status of the FSP. For people using the plan besides the FSO this page and the following Company Profile page could be very useful.

Month/Day/Year Initials

Month/Day/Year Initials

Month/Day/Year Initials

Month/Day/Year Initials

The plan is good for five years after the approval by the cognizant COTP. Then there will be a requirement for resubmission of the plan.

Facility Security Plan

COMPANY PROFILE

Date: _____

Company Name: ENTER YOUR COMPANY NAME.
Company Address: ENTER YOUR COMPANY'S PHYSICAL ADDRESS.
Company Address: ENTER YOUR COMPANY'S MAILING ADDRESS.
Facility Location: ENTER FACILITY LOCATION THAT THIS PLAN APPLIES TO.
General Manager: ENTER THE GENERAL MANAGER'S FIRST AND LAST NAME.
Primary POC: ENTER YOUR COMPANY'S PRIMARY POINT OF CONTACT.
Title: ENTER TITLE.
E-mail: ENTER E-MAIL ADDRESS.
Office: ENTER OFFICE PHONE NUMBER.
Home: ENTER HOME PHONE NUMBER.
Cell: ENTER CELLULAR PHONE NUMBER.
Secondary POC: ENTER YOUR COMPANY'S SECONDARY POINT OF CONTACT.
Title: ENTER TITLE.
E-mail: ENTER E-MAIL ADDRESS.
Office: ENTER OFFICE PHONE NUMBER.
Home: ENTER HOME PHONE NUMBER.
Cell: ENTER CELLULAR PHONE NUMBER.
Plan Completed By: ENTER NAME OF PERSON RESPONSIBLE FOR MAINTAINING THIS SECURITY PLAN.

***Note 1:** This page is included for the FSO to put all pertinent information. This quick reference card is a good idea but is not a required part of the FSP writing process. This information would be spread through the plan mostly in Section 1.*

***Note 2:** Definitions of MARSEC Levels and other pertinent terms in the Security Regulations are found in the definitions section of 33 CFR 101.105, details which add to the definition and are more specific are added within each subchapter. An example of this is the types of things that could be considered Restricted Areas in 33 CFR 105.260(b).*

Section 1. Security Administration and Organization

The facility owner or operator will identify those persons who will have duties and responsibilities with regards to security. Perhaps the most important such person will be the Facility Security Officer. Also necessary is identifying the structure of the security organization.

Document the qualifications required of the personnel serving in the security organization.

Identification of the owners and operators of the facility shall be included.

33 CFR 105.200 and 105.205 detail some of the information of an administrative nature that could be included here. This first section is primarily for points of contact and identifying the Chain of Command for actual incidents, drills and for passing information from the community at large to the facility.

Section 2. Personnel Training

Formal training and the certification of key personnel is required by the owners or operators of the facility for each person within the security organization.

The levels of training and the equivalents in experience are not specifically stated in the Regulations. Differences in requirements will depend on the type of facility, the size of the facility and other variables.

Certification of Vessel Security Officers, Company Security Officers and Facility Security Officers by approved training is being considered for future implementation. At the current time such standards do not exist. But this chapter has to list knowledge, experience and schooling that apply to the requirements of 33 CFR 105.

33 CFR 105.205, 105.210 and 105.215 all involve the training and qualification concepts for persons to be certified for the security organization positions.

Facility Security Plan

Section 3. Drills and Exercises

Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

A schedule of drills and exercises of a routine nature may be included. Drills work with small sections of the plan where exercises are full scale and may involve other facilities or groups with interest in security matters.

33 CFR 105.220 discusses the requirements for drills and exercises.

Facility Security Plan

Section 4. Records and Documentation

Records and documentation may be kept in the plan in this section or they may be kept on the facility and this section may index or reference the subjects and locations of the files. The actual records must be made available, upon request, to representatives from the CG who are authorized to act under the Security Regulations. Records are to be kept for two years.

Records on these topics must be kept by the FSO: (1) Training; (2) Drills and exercises; (3) Incidents and breaches of security; (4) Changes in MARSEC Levels; (5) Maintenance, calibration and testing of security equipment; (6) Security threats; (7) Declaration of Security; (8) Annual audit of the FSP.

33 CFR 105.225 details the record keeping requirements. Additionally, 33 CFR 105.120 dictates compliance documentation that should be kept in this section as well.

Section 5. Response to change in MARSEC Level

The Cognizant Coast Guard Authority will set Maritime Security (MARSEC) levels. Actions required at each level shall be in keeping with the regulations and shall be detailed in this section. MARSEC needs are defined more by the facility type and location than by any other feature.

This section will be general response. There are specific lists of things that should or shall be completed as MARSEC Levels increase within the regulations and specified in later sections of this plan. But, there are also changes to be considered as MARSEC Levels decrease.

33 CFR 101.105 & 101.200 definitions is a good place to start for MARSEC descriptions, setting levels. Then, 33 CFR 105.285, 105.290, 105.295 and 105.296 provide additional requirements for facilities of particular type.

Section 6. Procedures for interfacing with vessels

Checklists or Standard Operating Procedures or Quick Reference Cards should be developed for ship to shore contacts and working practices for each MARSEC level. This is with regards to security patrols and notifications and the like, and should be relatively simple. More intensive procedures for raised MARSEC levels and specific facilities will have the interface augmented by a Declaration of Security (see Section 7). The focus of this section of the FSP is the facilities procedures. The Declaration of Security will include within it the vessel responsibilities as well as facility responsibilities. A form similar to a Declaration of Inspection (regulations for such found in 33 CFR 156) may be used but must address all the Security Concerns of the MARSEC Level.

It would be wise to discuss in this section how much of the FSP will be available to the Vessel Security Officer and vessel security personnel. In general, this section should detail the role of vessel agents as well. Also, consider access to the facility by vessel personnel for phone calls or shore leave or other circumstances.

33 CFR 105.240 is the citation for the requirements of this section.

Section 7. Declaration of Security

A Declaration of Security (DoS) shall be implemented as required by regulation. This section should detail when and how to do a DoS as well as blank forms or an example of the verbiage for an agreement.

There are recommended forms for the vessel, which may cover the needs of the facility. As the agreement is executed and signed by both the Vessel Security Officer and the Facility Security Officer* it should be understandable, accurate and legible. This can mean a preprinted form or a letter developed on computer and printed.

** The Facility may designate persons other than the FSO to sign the DoS. The list of personnel acceptable by the facility to sign a DoS shall be a part of the FSP.*

33 CFR 101.105 states that a Declaration of Security is an agreement executed between the responsible Vessel and Facility Officers (in this case) that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time the vessel is moored to the facility. 33 CFR 105.245 discusses the requirements of a DoS for the facility.

Section 8. Communications

Communication equipment and content and methods are considered in this section. The ability to notify personnel involved in the facility's security and employees of changes in MARSEC are to be identified. Also the phone, radio, pager and intercom systems are to be addressed.

Communicating conditions to facility personnel in non-emergency and emergency situations is a requirement of this section. Also, equipment for communication is to be detailed and the procedures for the use of this equipment.

33 CFR 105.235 discusses the requirements of communications.

Section 9. Security systems and equipment maintenance

Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations. The FSP must include procedures for identifying and responding to security system and equipment failures or malfunctions as well as the routine schedules. Record keeping is required for these operations.

33 CFR 105.250 is very general. The equipment that works best for your facility will be determined by the needs of your facility and environment more than by regulation. The engineers and FSO who design the systems will have a large field of equipment to choose from and it is their responsibility to define the best system for their facility. Cameras, remote sensors, key card devices are all potentially useful. Yet they may not be feasible for every facility.

Section 10. Security measures for access control, including designated public access areas

The facility owner or operator must ensure the implementation of security measures to: deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports; secure dangerous substances and devices that are authorized by the owner or operator to be on the facility; and control access to the facility.

The facility owner or operator must establish in this plan the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

33 CFR 105.255 has a checklist of requirements for each MARSEC Level

Facility Security Plan

Section 11. Security measures for restricted areas

The facility owner or operator must ensure the designation of restricted areas in order to: prevent or deter unauthorized access; protect persons authorized to be in the facility; protect the facility; protect vessels using and serving the facility; protect sensitive security areas within the facility; protect security and surveillance equipment and systems.

The facility owner or operator must ensure restricted areas are designated within the facility. A few examples of restricted areas: shore areas immediately adjacent to each vessel moored at the facility; areas containing sensitive security information, including cargo documentation; or areas containing security and surveillance equipment and systems and their controls, and lighting system controls.

Security measures are items like: identifying which facility personnel are authorized to have access; determining which persons other than facility personnel are authorized to have access; and determining the conditions under which that access may take place.

At different MARSEC levels requirements will change. At MARSEC Level 1, the facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include: restricting access to only authorized personnel; or securing all access points not actively used and providing physical barriers to impede movement through the remaining access points. In addition to the security measures required for MARSEC Level 1, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in this plan. These additional security measures may include: increasing the intensity and frequency of monitoring and access controls on existing restricted access areas; or enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices. Again there are increases in security at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified in this plan. These additional security measures may include: restricting access to additional areas; prohibiting access to restricted areas, or searching restricted areas as part of a security sweep of all or part of the facility.

33 CFR 105.260 contains the requirements for this section.

Facility Security Plan

Section 12. Security measures for handling cargo

The facility owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to: deter tampering; prevent cargo that is not meant for carriage from being accepted and stored at the facility; identify cargo that is approved for loading onto vessels interfacing with the facility; include cargo control procedures at access points to the facility; identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up; restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate; ensure the release of cargo only to the carrier specified in the cargo documentation; coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures; create, update, and maintain a continuous inventory, including location, of all dangerous goods or hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods or hazardous substances; and be able to **check cargo** entering the facility for dangerous substances and devices at the rate specified in this plan. Means to check cargo include: visual examination; physical examination; detection devices, such as scanners; or canines.

At the different MARSEC Levels there are specific requirements within the regulations. Checklists, procedures and definitions of routine are what this plan is going to require.

33 CFR 105.265 defines the needs at specific MARSEC Levels.

Section 13. Security measures for delivery of vessel stores and bunkers

The facility owner or operator must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to: check vessel stores for package integrity; prevent vessel stores from being accepted without inspection; deter tampering; for vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and check vessel stores by the means defined previously for checking cargo.

The regulation cited below has the requirements at the different MARSEC Levels. This section of your plan, as with the others will detail in checklists and operating procedures how your facility will fulfill the regulatory list

33 CFR 105.270

Section 14. Security measures for monitoring

The facility owner or operator must ensure the implementation of security measures that have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, and automatic intrusion-detection devices, or surveillance equipment, as specified in this plan the: facility and its approaches, on land and water; restricted areas within the facility; and vessels at the facility and areas surrounding the vessels.

The monitoring of perimeter and conditional increases for each MARSEC Level shall be defined in this section of the plan. The personnel requirements, the equipment and the patrols are to be considered and addressed in this section of the plan.

33 CFR 105.275 has the elements that are required for monitoring, and ties into the Section 9 Equipment Chapter..

Section 15. Security incident procedures

This section of the plan shall how the facility shall, for each MARSEC Level, ensure the FSO and facility security personnel are able to: respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations; evacuate the facility in case of security threats or breaches of security; report security incidents as required in 33 CFR 101.305; brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and secure non-critical operations in order to focus response on critical operations.

33 CFR 105.280

Section 16. Audits and security plan amendments

Amendments to the plan will occur only after there is an approved plan on file. This is true of audits as well. Amendments have specific timelines for submission and approval, based on whether they are initiated by the COTP or by the facility. Audits will take place beginning one year after approval and shall be done annually.

33 CFR 105.415 discusses in detail the variations that are applicable to these two elements which are designed to keep the plan current and effective.

Section 17. Facility Security Assessment (FSA) report

The scope of the Facility Security Assessment is discussed in Subpart C of the interim final rule. The report is a collection of background information, an on scene survey and an analysis of that information. The report is to be completed and submitted with the FSP. The requirement is to Risk Based Decision Making in the assessment process. Examples of assessment tools exist in regulations see 33CFR101.510 all.

This link is to an article on Risk Based Decision Making. While not endorsed as the only RBDM out there it is an example of what can be found with a simple search on the Internet. This article can give an adequate introduction to the process.

<http://www.rdc.uscg.gov/Reports/risk-qrg.pdf>

33 CFR 105.300 through 310 discuss the Facility Security Assessment and submission requirement.

Section 18. Facility Vulnerability and Security Measures Summary.

The Federal Register has a copy of form CG-6025. This form is to be completed and included with the FSP. The information in the FSP and from the FSA will be used to complete this form.

33 CFR 105.405(a)(18) and 33 CFR 105.405(c) have the details and the form is listed as Appendix A to Part 105.